



**Canadian Forum for Digital Infrastructure (CFDIR)
Artificial Intelligence / Machine Learning (AI/ML)
Working Group (WG)**

**SOVEREIGN AI
INFRASTRUCTURE RESILIENCE
DISCUSSION PAPER**

Version 2.0: 2026 June 1



**AUTHORED BY:
AI/ML WG
of the Canadian Forum for Digital Infrastructure Resilience (CFDIR)**

TLP: CLEAR

SOVEREIGN AI INFRASTRUCTURE RESILIENCE

The contents of this document are **TLP:CLEAR**

Reproduction is authorized provided the source is acknowledged.



CONTENTS

Contents.....	iii
Foreword.....	iv
Acknowledgements.....	v
CFDIR Members:.....	v
Revision History	vi
1. Executive Summary.....	1
2. Introduction	2
3. Why AI Sovereignty matters	3
4. GOALS : Control ; Resilience ; Standards Of Practice.....	4
4.1 Goal 1 : Control	4
4.2 Goal 2 : Resilience.....	4
4.3 Goal 3 : Standards Of Practice	4
5. Technology Framework (Stack View and Sovereign Controls)	5
5.1 Infrastructure Layer	5
5.2 Data Layer	5
5.3 Model Development Layer	5
5.4 Deployment and Operations Layer (MLOps).....	6
5.5 Governance and Assurance Layer	6
5.6 Application Layer	6
6. People Considerations	7
7. Policy Recommendations.....	8
8. Process Considerations	9
9. Case Studies : International Approaches and Lessons	10
10. Call to Action	11
10.1 Immediate Recommendations (12 – 18 Months).....	11
10.2 Long Term Strategy (2 – 5 Years).....	11
11. Conclusion.....	12
Annex A: Glossary.....	13

FOREWORD

The contents of this document were developed during the course of Canadian Forum for Digital Infrastructure (CFDIR) Artificial Intelligence / Machine Learning (AI/ML) Working Group meetings, from 2025 April – 2026 January.

ACKNOWLEDGEMENTS

The information and recommendations contained herein were informed by the active participation and engagement of subject matter experts from the following organizations (listed alphabetically):

CFDIR MEMBERS:

Industry:

- BlackBerry
- Dell
- IBM Canada
- Oracle
- Thales Canada

Government:

- Canadian Centre for Cyber Security (CCCS)
- Innovation, Science, and Economic Development (ISED) (CFDIR Secretariat)
- Public Safety Canada (PS)

REVISION HISTORY

The following table describes the dates of the major changes to this document.

Authors	Date	Version	Notes
CFDIR AI/ML WG	2026 January 15	Version 1.0	First Release
ISED	2026 June 1	Version 2.0	Document Formatting

1. EXECUTIVE SUMMARY

Canada's AI sovereignty is fundamentally a resilience agenda: protect what matters most including Canadian highly productive technology economic activities, reduce single points of failure, and ensure essential AI capabilities remain available, controllable, and aligned with Canadian law and values. Sovereignty requires practical control across six pillars: data, infrastructure, operations, technological origin/supply chain, freedom to choose (solution choice), and legal jurisdiction, implemented with risk-based priorities and engineered redundancy.

Over-reliance on a few foreign-owned compute and AI capabilities creates geopolitical, operational, and legal exposure. Canada should retain credible sovereign options for critical workloads (defence, public safety, health, and critical infrastructure), while remaining open to collaborate with trusted global partners increasing choice and innovation. Resilience must be deliberately engineered across the AI stack: diversified suppliers; failover pathways including domestic edge modes; high-availability architectures; red teaming and safety testing; and continuity plans exercised under realistic stress scenarios.

Immediate actions (12–18 months) include standing up Canadian-controlled sovereign compute; codifying data residency and training/inference location for sensitive data; mandating Canada based and operated Security Operations and Model Operations Centers (SOC/MOC) for critical workloads; adopting open architectures to preserve portability and vendor diversity; establishing Responsible AI Certification for critical infrastructure; integrating continuity planning and sovereign failover into departmental AI strategies; launching a bilingual plus Indigenous-language data program; and embedding 'sovereignty and resilience' clauses in major AI procurements.

2. INTRODUCTION

This paper provides a focused route map for asserting AI sovereignty where it matters most. It identifies the choke points Canada must control, where global interdependence is acceptable as long as it supports governments agenda for a stronger Canada, and how to structure governance to balance central oversight with local autonomy. It draws upon working group contributions and a draft discussion paper to distill actionable measures for Government of Canada decision-makers.

3. WHY AI SOVEREIGNTY MATTERS

Canada operates in a global digital ecosystem dominated by concentrated cloud, silicon, and model providers. Sovereignty is the practical capability to guarantee access, control, and lawful operation of AI systems that underpin critical services while ensuring that such activities have a meaningful contribution to the economy of Canada and our leadership role in AI around the world. The question is not whether to collaborate globally - we should - but which parts of the AI stack must remain sovereign to assure safety, continuity, and compliance with Canadian law in times of stress.

Push factors include geopolitical and jurisdictional risk, market concentration, talent and infrastructure leakage, and systemic vulnerability to outages. Pull factors include the ability to encode Canadian values and bilingual/Indigenous contexts in models, build domestic industry and long-term ownership, and maintain strategic room to maneuver through credible control of essential building blocks.

4. GOALS: CONTROL; RESILIENCE; STANDARDS OF PRACTICE

4.1 GOAL 1: CONTROL

Control is end-to-end across the AI stack: data, compute, models, pipelines, and operations. Canada must be able to authorize, operate, and adapt critical AI capabilities on demand, without external coercion. Concretely: **(1) data sovereignty** includes residency, authorized access, compliance with sector-specific laws; **(2) infrastructure sovereignty** includes Canadian-located and Canadian-controlled compute, storage, networking, and facilities; **(3) operations sovereignty** includes Canadian-operated SOC/MOC, incident response, and change control; **(4) technological sovereignty** includes strategic ownership of IP where it matters, with risk-based use of foreign tech; **(5) solution sovereignty** includes procurement leverage and open architectures to preserve freedom of choice; and **(6) legal sovereignty** includes keeping sensitive workloads under Canadian jurisdiction.

4.2 GOAL 2: RESILIENCE

Resilience means engineered continuity across suppliers, regions, and architectures. For AI, it includes sovereign failover paths, domestic edge modes that sustain essential services during disconnection, stress-tested high-availability designs, diverse model/compute options, and routine exercises (including red teaming) to validate recovery under realistic scenarios. Resilience must explicitly extend to rural, remote, and Indigenous communities so that essential AI-enabled public services are reliable nationwide.

4.3 GOAL 3: STANDARDS OF PRACTICE

Standards codify security, privacy, ethics, transparency, auditability, bilingual and Indigenous-language support, accessibility, and incident response. They should be risk-based and sector-specific, interoperable with allied frameworks, and embedded into procurement and certification. Responsible AI assurance should include documented model provenance, safety testing (alignment, robustness, reliability), monitoring, incident reporting, and post-incident learning.

5. TECHNOLOGY FRAMEWORK (STACK VIEW AND SOVEREIGN CONTROLS)

A clear, layered view of the AI technology stack helps identify where sovereignty is essential and where global interdependence can be leveraged. Each layer, from infrastructure to applications, including operations and monitoring, requires specific measures to ensure sovereignty, resilience, and lawful control.

5.1 INFRASTRUCTURE LAYER

At the foundation, Canada must guarantee Canadian-controlled capacity for critical workloads. This means deploying data centers located within Canada, establishing dedicated sovereign regions or clusters, infrastructure operations must be restricted to only Canadian-approved persons located in Canada, and ensuring robust physical security, power, and cooling. Supply diversification for GPUs and accelerators is critical to avoid dependency on single vendors. Networking should be low-latency and resilient, ideally supported by private backbones, while hardware and firmware must be validated for integrity. Preparing for quantum-safe cryptography and implementing standardized observability across systems will further strengthen this layer.

5.2 DATA LAYER

Sensitive data must remain under Canadian jurisdiction, with transparent governance and auditable lineage. Residency and processing controls should apply to both training and inference stages. Data Layer operations must be restricted to only Canadian-approved persons located in Canada. Strong identity and access management, encryption, and privacy-preserving techniques are essential. Sector-specific compliance such as health, defence, and Indigenous data governance must be enforced, alongside portable schemas to prevent vendor lock-in.

5.3 MODEL DEVELOPMENT LAYER

Canada needs the ability to train, fine-tune, and evaluate models aligned with Canadian contexts. This includes running sensitive training operations domestically, leveraging transfer learning with Canadian datasets, and maintaining documented model cards and evaluations. Rigorous safety, robustness, and bias testing should be standard, complemented by reproducible pipelines and red-teaming exercises. Strategic retention of intellectual property for domain-specific models will

SOVEREIGN AI INFRASTRUCTURE RESILIENCE

ensure long-term sovereignty. For this layer, Canadian approved Operations should only be used to support sovereign control.

5.4 DEPLOYMENT AND OPERATIONS LAYER (MLOPS)

Reliable operation under Canadian authority is non-negotiable. Sovereign control should extend to containerization, orchestration, autoscaling, and secure CI/CD pipelines. Canadian-operated Security and Model Operations Centers (SOC/MOC) must oversee runtime monitoring, incident response, and change control. Failover mechanisms and domestic edge modes should be integrated to maintain continuity during disruptions. For this layer, Canadian approved Operations should only be used to support sovereign control.

5.5 GOVERNANCE AND ASSURANCE LAYER

This layer codifies lawful, ethical, and resilient operation. Responsible AI certification for critical infrastructure should mandate safety testing, alignment evaluations, and incident reporting. Audit trails, third-party conformity assessments, and openness requirements for portability are essential. Governance must also embed bilingual and Indigenous-language support and ensure transparency proportionate to risk. For this layer, Canadian approved Operations should only be used to support sovereign control.

5.6 APPLICATION LAYER

Trusted AI-enabled public services must be delivered with safeguards. Domain-specific validation such as for health triage or emergency response should be routine. Accessibility and human-in-the-loop mechanisms are vital for consequential decisions, with fallback procedures ready when AI systems degrade or fail. For this layer, Canadian approved Operations should only be used to support sovereign control.

6. PEOPLE CONSIDERATIONS

AI sovereignty is deeply human. Policies must recognize that people create, operate, and are impacted by AI systems. A sovereign approach begins with mapping stakeholders across the lifecycle - Data Subjects (whose data is used), Data Makers (who input and curate data), Decision Makers (who rely on AI for decisions), and Decision Subjects (those affected by those decisions) - and extends to Dependents and System Influencers such as regulators, vendors, and advocacy groups.

Policies should mandate early user research, iterative design with guardrails, and documented accountability for decisions. Red teaming exercises and risk forecasting must be routine to anticipate second- and third-order effects before deployment. Workforce development is critical: Canada needs talent pipelines for AI engineers, governance specialists, and Indigenous-led innovation hubs to ensure inclusivity and nationwide reliability, including rural and northern communities.

Practical measures: require stakeholder maps and impact assessments at project inception; designate accountable owners for AI risks within each department; embed human-in-the-loop controls for consequential decisions; and exercise continuity plans that include sovereign failover and edge modes.

7. POLICY RECOMMENDATIONS

Canada should define sovereignty as autonomy and control over critical AI technologies and data while remaining open to global innovation. Policies must promote client choice and flexibility, supporting on-premises, hybrid, and cloud models to avoid lock-in and preserve portability.

Invest in national capacity: stand up Canadian-controlled sovereign compute; fund bilingual and Indigenous-language datasets and tuning programs; and retain IP for domain-specific models where strategically important. Establish a Responsible AI Certification for critical infrastructure that mandates safety testing, robustness checks, alignment evaluations, continuous monitoring, incident reporting, and post-incident learning.

Require open architectures with portable schemas and APIs to enable multi-vendor interoperability across data and AI pipelines. Apply risk-based localization—codifying residency and processing controls for sensitive data and workloads, rather than blanket requirements. Foster public–private collaboration through sandboxes, joint exercises, and shared standards aligned with allied frameworks.

Embed sovereignty and resilience clauses in procurement: data residency, supply-chain transparency, Canadian-operated SOC/MOC for critical workloads, and explicit failover paths including domestic edge capabilities.

8. PROCESS CONSIDERATIONS

Effective governance processes are as important as technology. Define clear roles and oversight mechanisms, with named risk owners responsible for identifying, mitigating, and reporting AI risks. Establish transparent codes of conduct and structured mechanisms for change control under Canadian authority.

Integrate stress testing and continuity planning: simulate outages, supplier failures, and geopolitical shocks; validate sovereign failover paths and edge modes; and run regular exercises including red teaming. Maintain dynamic standards for security, privacy, ethics, accessibility, and auditability, updated to reflect technological and geopolitical change and extend sovereign capabilities to rural, remote, and Indigenous communities.

Institutionalize incident reporting and learning: mandate post-incident reviews, publish proportionate transparency reports, and incorporate lessons into standards and procurement.

9. CASE STUDIES: INTERNATIONAL APPROACHES AND LESSONS

EU GAIA-X shows how sovereignty can be achieved through federated, interoperable cloud/data ecosystems using contractual and technical controls to enforce data location, portability, and European standards rather than reliance on a single vendor.

The UK's Sovereign Cloud illustrates dedicated sovereign regions for public sector and defence with domestic control of operations and monitoring, interconnected by resilient private backbones to enable high availability and disaster recovery while leveraging hyperscalers capabilities.

Estonia highlights cyber resilience via standardized e-government platforms, defensive automation, close partnerships (e.g., CCDCOE), and continuous exercises demonstrating that even small states can achieve high reliability through disciplined architecture and readiness.

Lessons for Canada: combine technical isolation for sensitive workloads (sovereign compute and edge modes), federated governance for interoperability, supplier diversity to reduce single points of failure, and institutionalize readiness through regular exercises and certification.

10. CALL TO ACTION

Issue a Government of Canada directive on AI sovereignty for critical workloads; stand up sovereign compute clusters; mandate data residency and sovereign operations for Canadian data; create Responsible AI Certification; embed open architecture in procurement; require sovereignty and resilience clauses in contracts; and institutionalize incident reporting and red teaming for critical systems.

10.1 IMMEDIATE RECOMMENDATIONS (12 – 18 MONTHS)

1. Sovereign Compute: Deploy Canadian-controlled GPU/accelerator capacity for priority sectors; establish domestic edge clusters for emergency failover.
2. Data Residency & Processing: Codify and enforce training/inference location and access controls for sensitive datasets under Canadian law.
3. Sovereign Operations: Require Canada based operation of SOC/MOC with 24/7 coverage, playbooks, and incident drills.
4. Open Architectures: Enforce portability and multi-vendor interoperability in data and AI pipelines; avoid lock-in through open schemas/APIs.
5. Responsible AI Certification: Mandate safety testing, alignment evaluations, robustness checks, and incident reporting for AI used in critical infrastructure.
6. Continuity Planning: Integrate sovereign failover and edge modes into departmental AI strategies; run regular exercises.
7. Bilingual + Indigenous-Language Data: Launch curated datasets and fine-tuning programs to adapt models to Canadian contexts.
8. Procurement Clauses: Include sovereignty/resilience requirements, supply-chain transparency, and access control guarantees in contracts.

10.2 LONG TERM STRATEGY (2 – 5 YEARS)

Scale sovereign compute, storage, and networking to frontier model needs; advance quantum-safe encryption and model reliability testing; institutionalize Responsible AI Certification; expand domestic talent pipelines and retention incentives; grow Canadian IP in domain models; and maintain interoperability with allied standards while anchoring sensitive workloads domestically.

11. CONCLUSION

AI sovereignty for Canada is about engineered resilience and lawful control over the capabilities that matter most. With focused investments, pragmatic standards, and risk-based governance, Canada can remain open to global innovation while anchoring critical services to a resilient Canadian foundation.

ANNEX A: GLOSSARY

AI	Artificial Intelligence
AI SI	AI Sovereign Infrastructure
CCI	Canadian Critical Infrastructure
CFDIR	Canadian Forum for Digital Infrastructure Resilience
GPU/TPU/NPU	Accelerators for AI Workloads
LLM	Large Language Model
MLOps	Machine Learning Operations
OT	Operational Technology
SOC/MOC	Security Operations Centre / Model Operations Centre

SOVEREIGN AI INFRASTRUCTURE RESILIENCE



This document is planned to be updated periodically, to reflect feedback and comments from implementing the information described herein.

TLP:CLEAR

Prepared by the AI/ML Working Group of the Canadian Forum for Digital Infrastructure Resilience (CFDIR)

Reproduction is authorized provided the source is acknowledged.